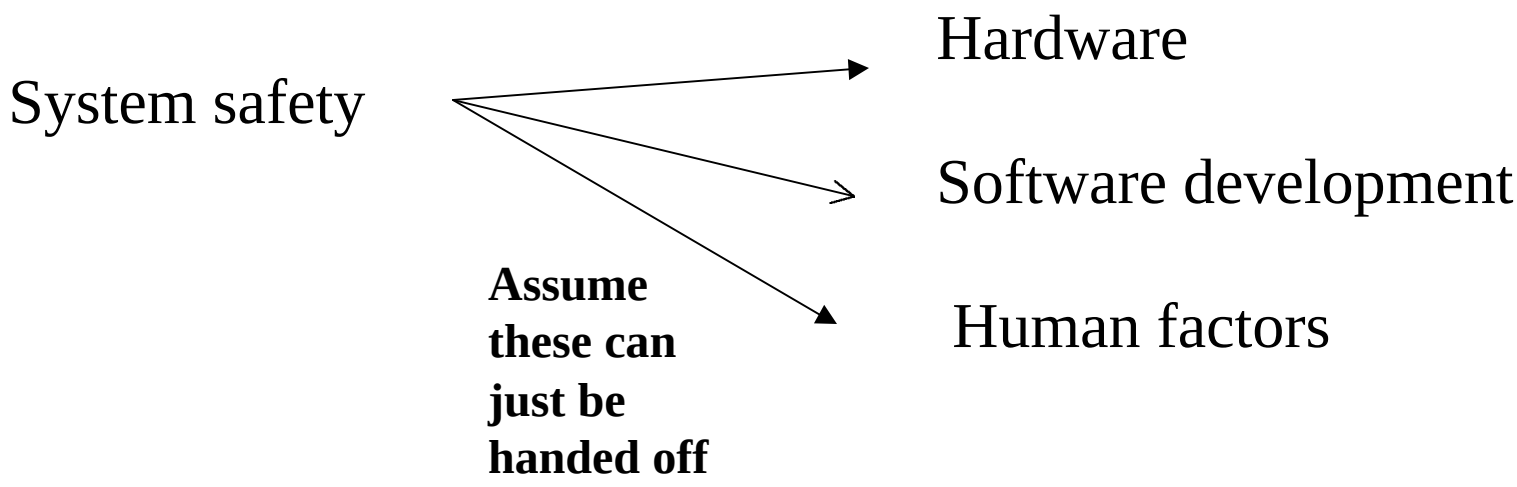
REPORT

Intent

- What questions need to be asked?
- What further data collection needs to be done?

Issues

- Need to talk about software, hardware, people, and systems.
  - Not integrating software and system processes
- Agency and industry need to learn the system safety process
  - includes hazard “handling” review
- Industry approaches have been very effective, but are conditions changing
  - complexity increasing rapidly
  - techniques becoming outdated



Approaches to safety

- SSA identifies the software level and perform good software development (178)
  - level is adequate
- Hazard-directed software development and analysis (882)
  - hardware failed
  - software sent incorrect variable
- SAE ARP4754, 4761
  - could provide input into 178B activities
  - reliability driven-software does not fail

Recommendations

- Workshop on applying system safety to software. (must be cost effective!) [FAA, INDUSTRY, OTHER ENTITIES]
  - Focus group on relationship between SSA and DO-178B
  - Define best practices (eg, 882, safety design) for incorporation into development standards.
    - Identify alternate means of best practices.
    - Notice emphasizing the scope of DO-178B and interfaces.
    - Training on SSA process
- Collection of software incidence and accidents data as contributing to system failure.